Srishyla Educational Trust (R)
GM INSTITUTE OF TECHNOLOGY
Approved by AICTE | Affiliated to V.T.U.Belgaum | Recognized by Govt. of Karnataka
NATIONAL BOARD OF ACCREDITATION
Accredited Programs
CSE/ECE/CE/ME

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

SEMINAR ACTIVITY

COURSE: FILE STRUCTURES **DATE: 10/07/2023**

SUBJECT CODE:18IS61

TOPIC: SIMPLE HASHING ALGORITHM

FROM: ADARSH DC **USN:4GM20IS002**

DESCRIPTION ABOUT TOPIC:

A simple hashing algorithm is a mathematical function that takes input data and produces a fixed-size output, typically a string of characters or a numerical value. The purpose of a hashing algorithm is to convert arbitrary input data into a unique or near-unique representation called a hash value or hash code. The hash code is typically a shorter representation of the original data and is used for various purposes, including data integrity checks, data indexing, and password storage.

ONE PARAGRAPH DETAIL ABOUT TOPIC:

Certainly! Here's a detailed explanation of a simple hashing algorithm:

Input Data: The algorithm takes an input data, which can be any type of data, such as a string, a number, or a file.

Convert Data to Binary: To process the input data, it needs to be converted into binary format. This step assigns a unique binary representation to each character or element in the input data. For example, in ASCII encoding, each character is represented by a unique 8-bit binary code.

Summing or Accumulating: The algorithm starts by summing or accumulating the binary representation of each character or element in the input data. This process involves adding up the binary values of all the characters or elements. The accumulated value serves as an intermediate representation of the input data.

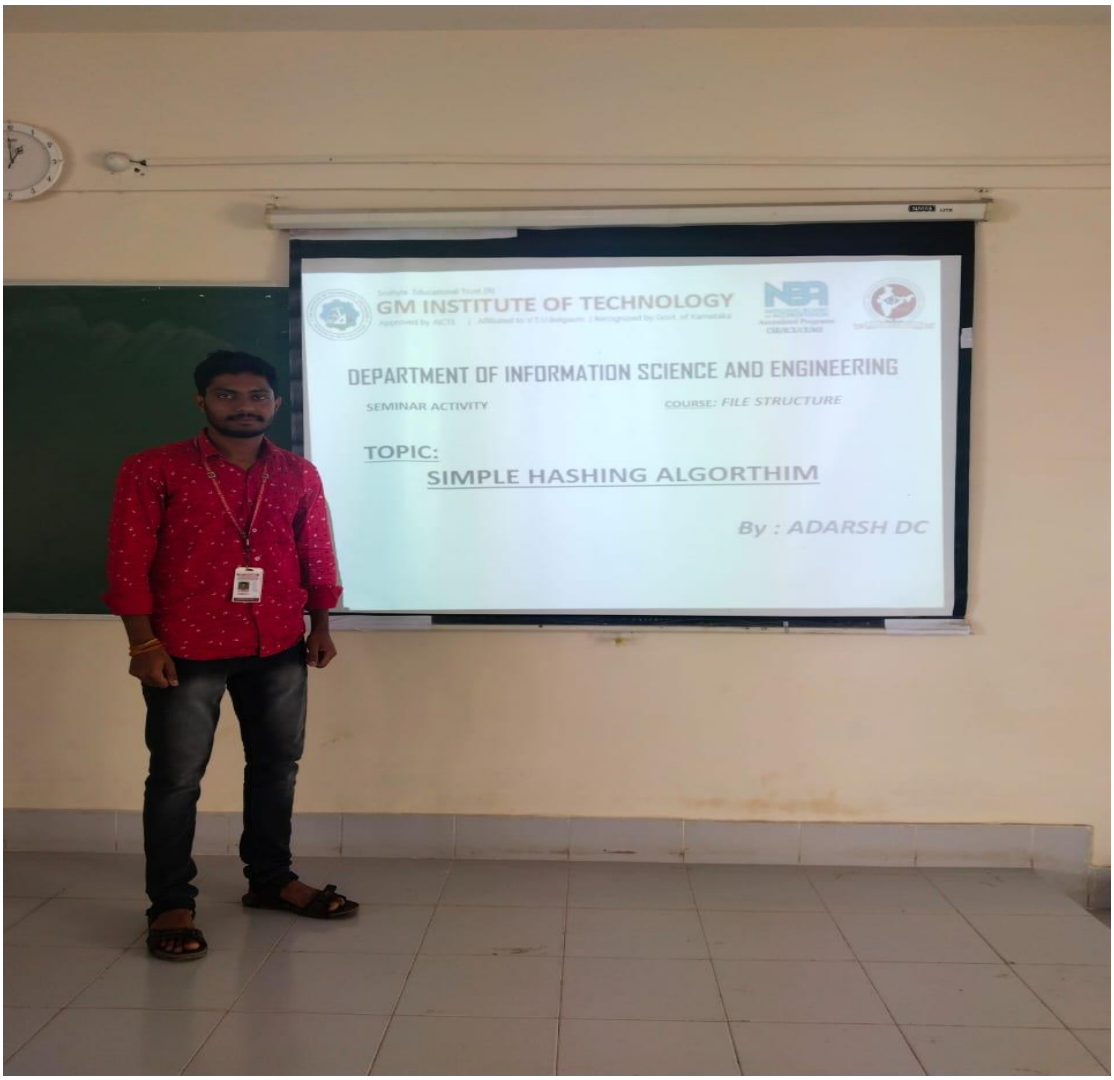
Modulo Operation: After accumulating the binary values, the algorithm applies a modulo operation. The modulo operator (%) returns the remainder of a division. By performing modulo operation, the algorithm ensures that the resulting hash value falls within a specific range or size.

Final Hash Value: The remainder obtained from the modulo operation becomes the final hash value. This hash value is typically represented as a hexadecimal or decimal number, or as a string of characters.

It's important to note that this simple hashing algorithm has limitations and is not suitable for security-related purposes. It may have a higher chance of collisions (different inputs producing the same hash value) due to its simplicity. Additionally, it lacks the properties of cryptographic hashing algorithms, such as resistance to pre-image attacks or the avalanche effect. Simple hashing algorithms are primarily used for non-security-critical tasks or simple data indexing purposes.

To ensure stronger security and resistance against attacks, it is recommended to use well-established cryptographic hashing algorithms, such as MD5, SHA-1, SHA-256, or bcrypt. These algorithms are designed with specific security properties in mind and have undergone extensive analysis and scrutiny by the security community.

IMAGE:



STUDENT SIGNATURE
ADARSH DC

SUBJECT COORDINATOR
DR.NEELAMBIKE S